Web Exercises
Part 3: Session Stealing

Barton P. Miller

Computer Sciences Department
University of Wisconsin

bart@cs.wisc.edu

Elisa Heymann

Computer Sciences Department
University of Wisconsin
Universitat Autònoma de Barcelona

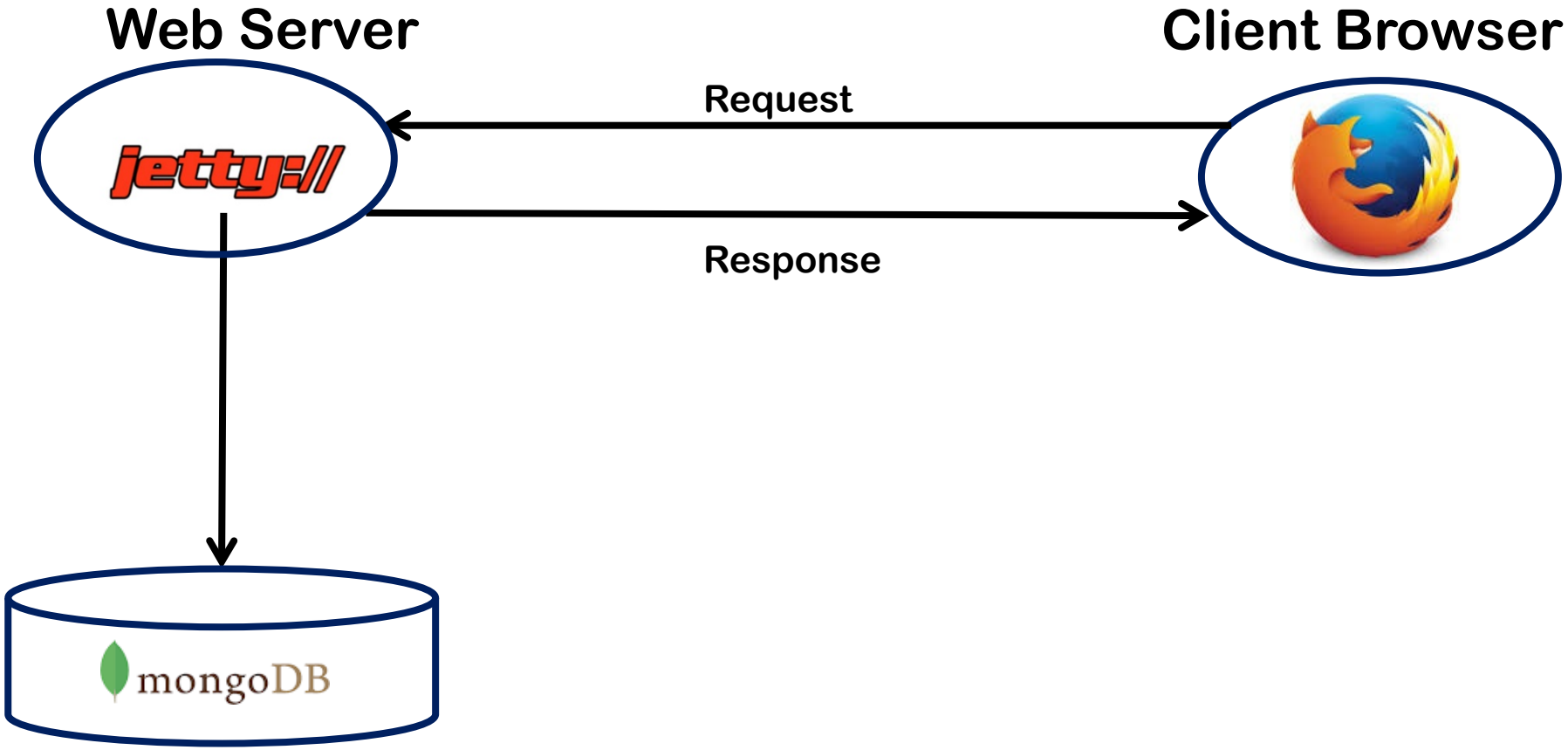
elisa@cs.wisc.edu

THE UNIVERSITY of WISCONSIN MADISON
Universitat Autònoma de Barcelona
TRUSTED CI THE NSF CYBERSECURITY CENTER OF EXCELLENCE

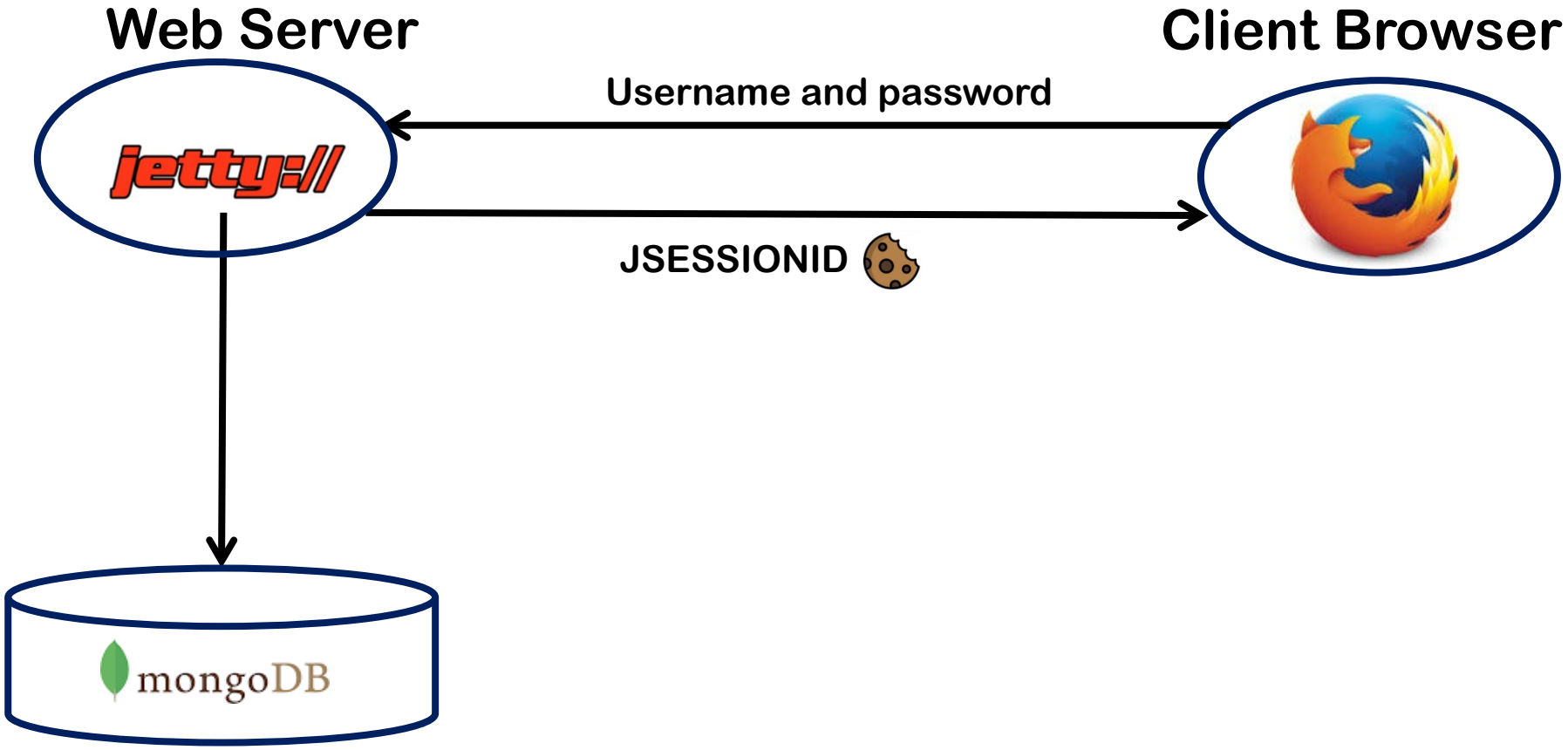
WisClick. Our Web Application

- A simple game.
  - Players click on a button to earn credits.
  - Users can manage their profiles.
  - Users can transfer (some of) their credits to others.
  - There is a top five ranking.
  - Users can view other users' page through the top five ranking.
- Vulnerable to web attacks.
- Exploit those vulnerabilities.

WisClick



WisClick


Web Server
Client Browser
Username and password
jetty://
JSESSIONID
mongoDB

WisClick. Our web application

You will use two accounts:

username: attacker
password: theattacker

username: victim
password: thevictim

To reset the database at anytime run:

```
cd ~/Web_Attack/src
mongo ResetMongo.js
```

Run WisClick

On a console run the web server:

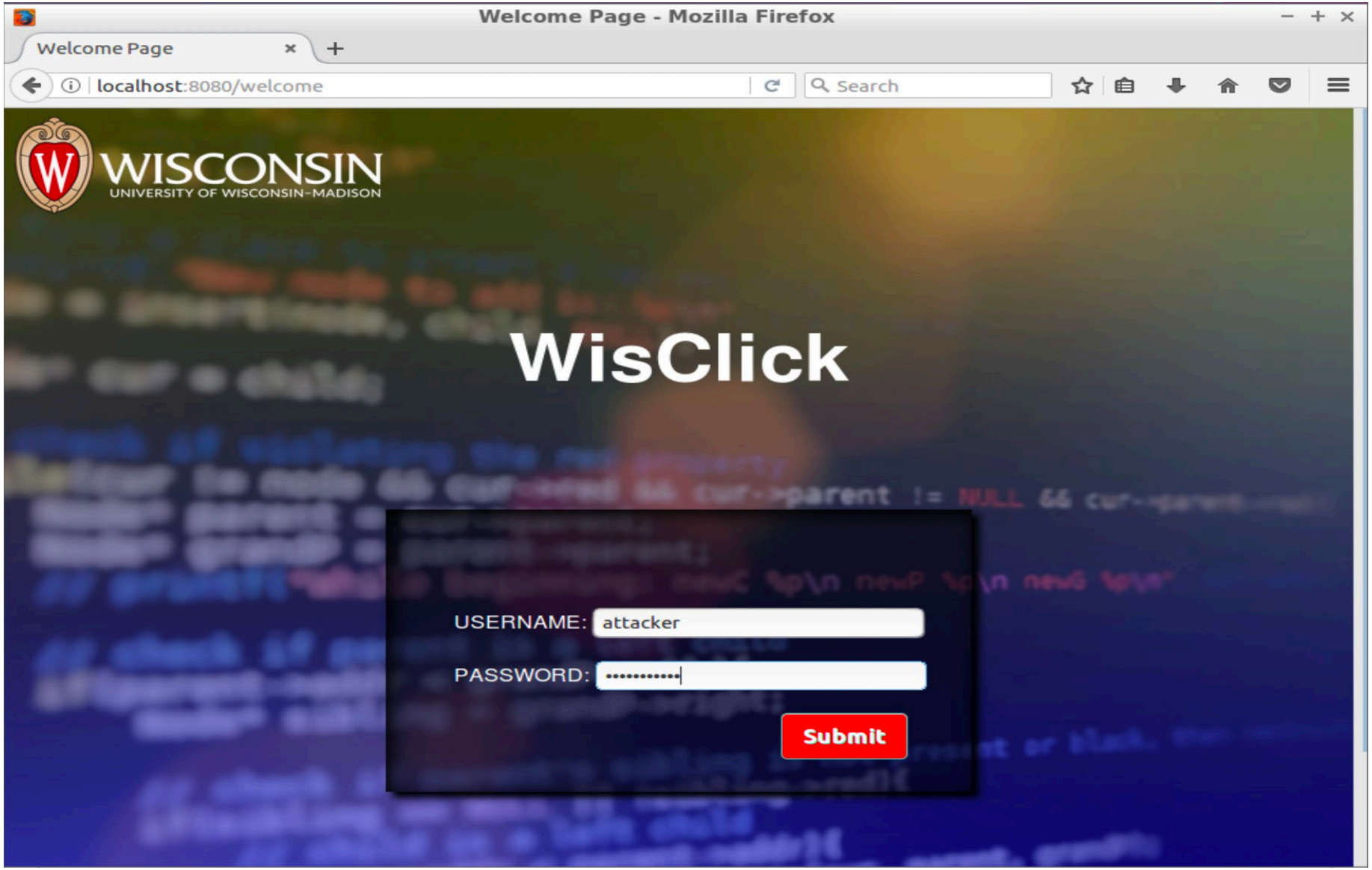
```
cd Web_Attack
ant
cd build/classes
./run.sh
```

On your web browser go to:

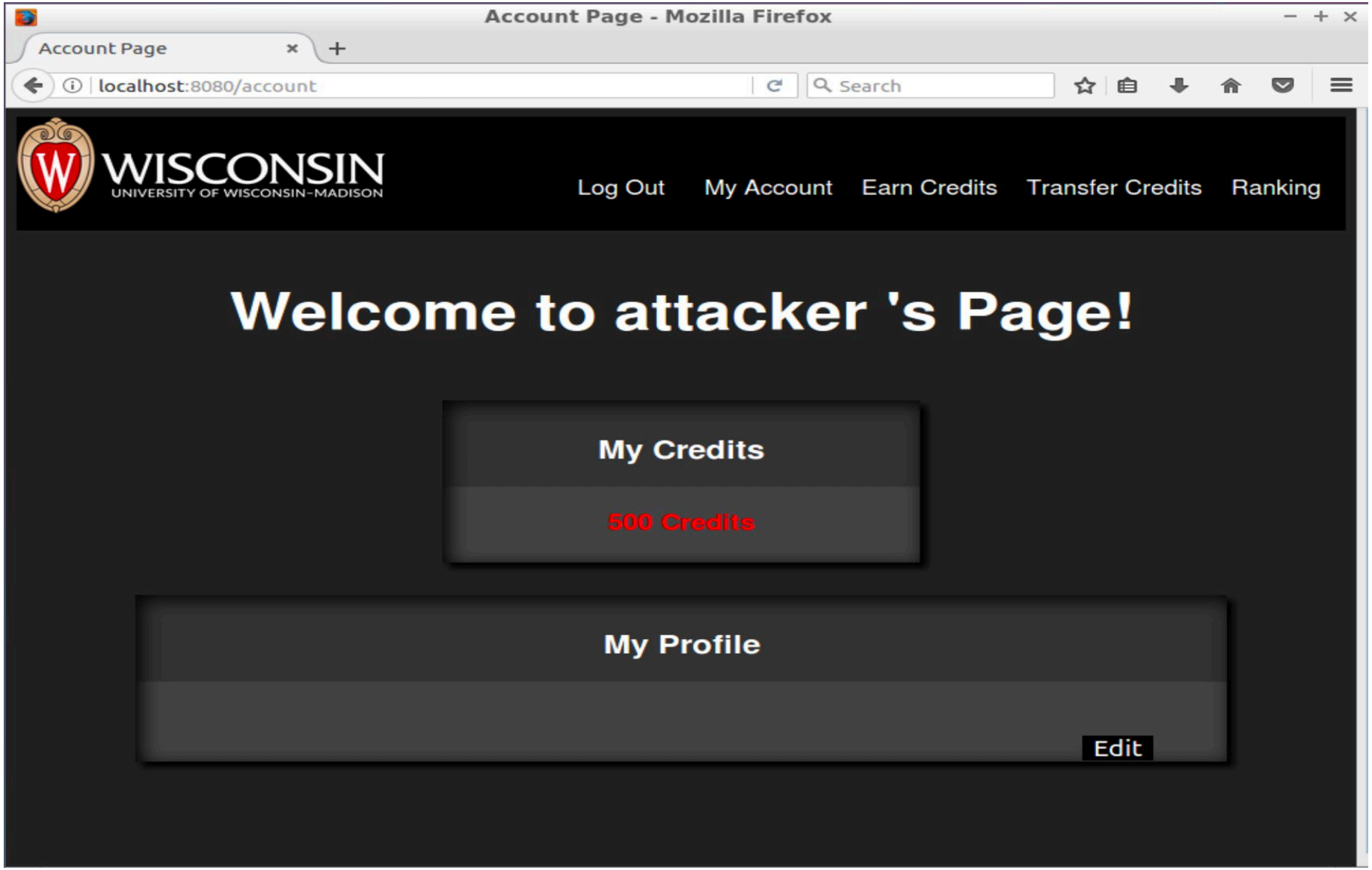
```
http://localhost:8080/welcome
```

Get familiar with the application:

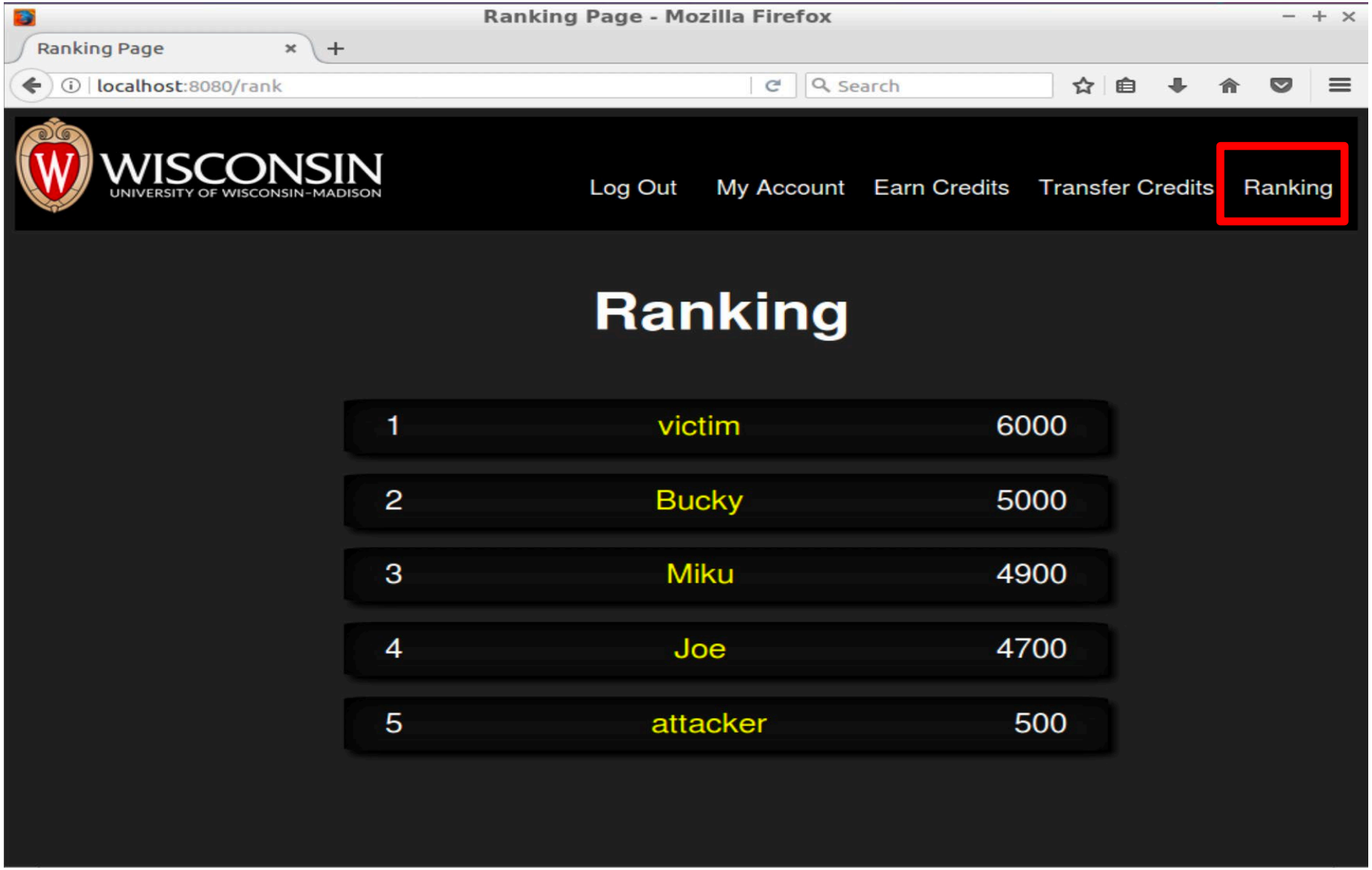
Run WisClick



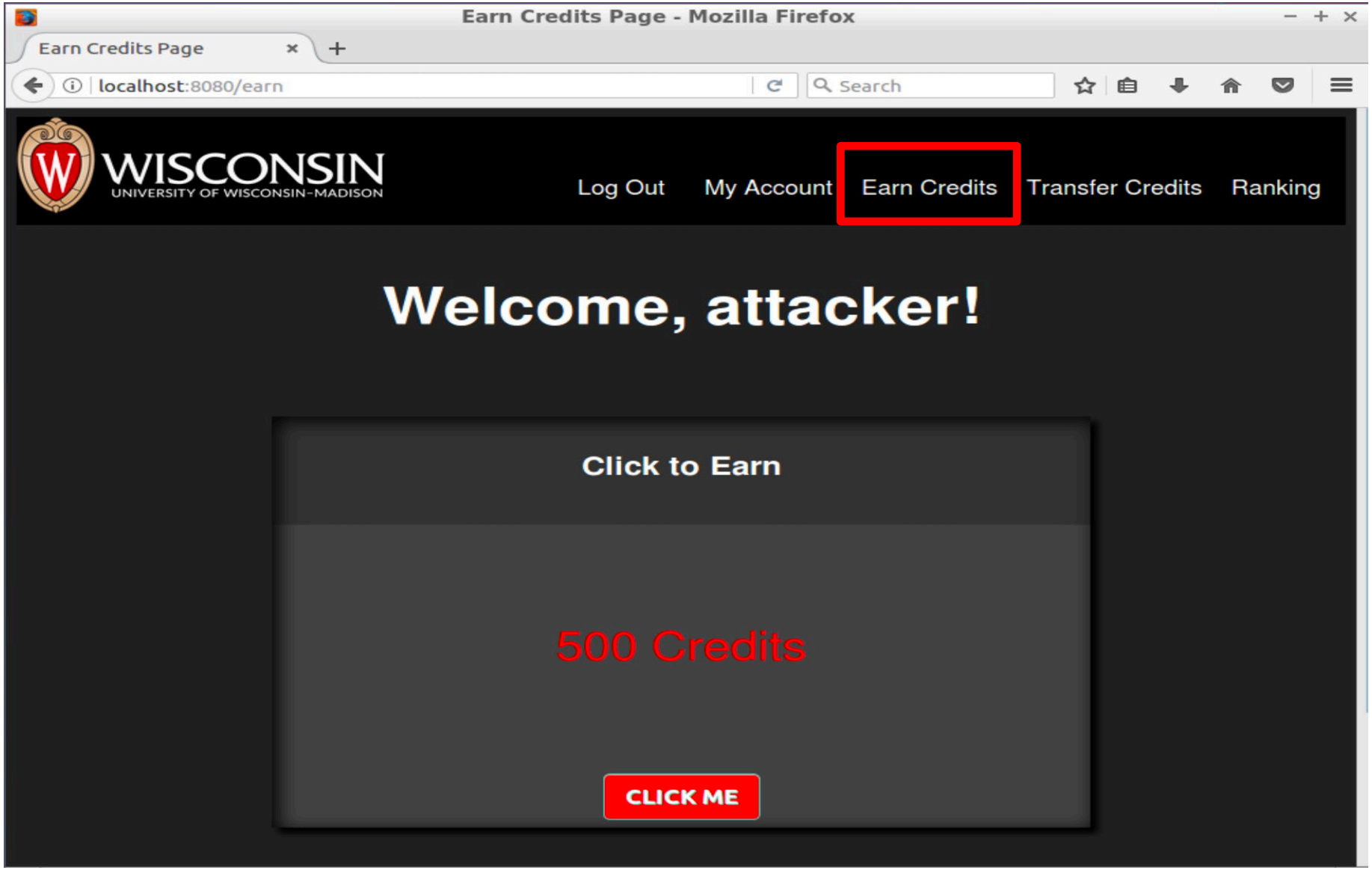
Run WisClick



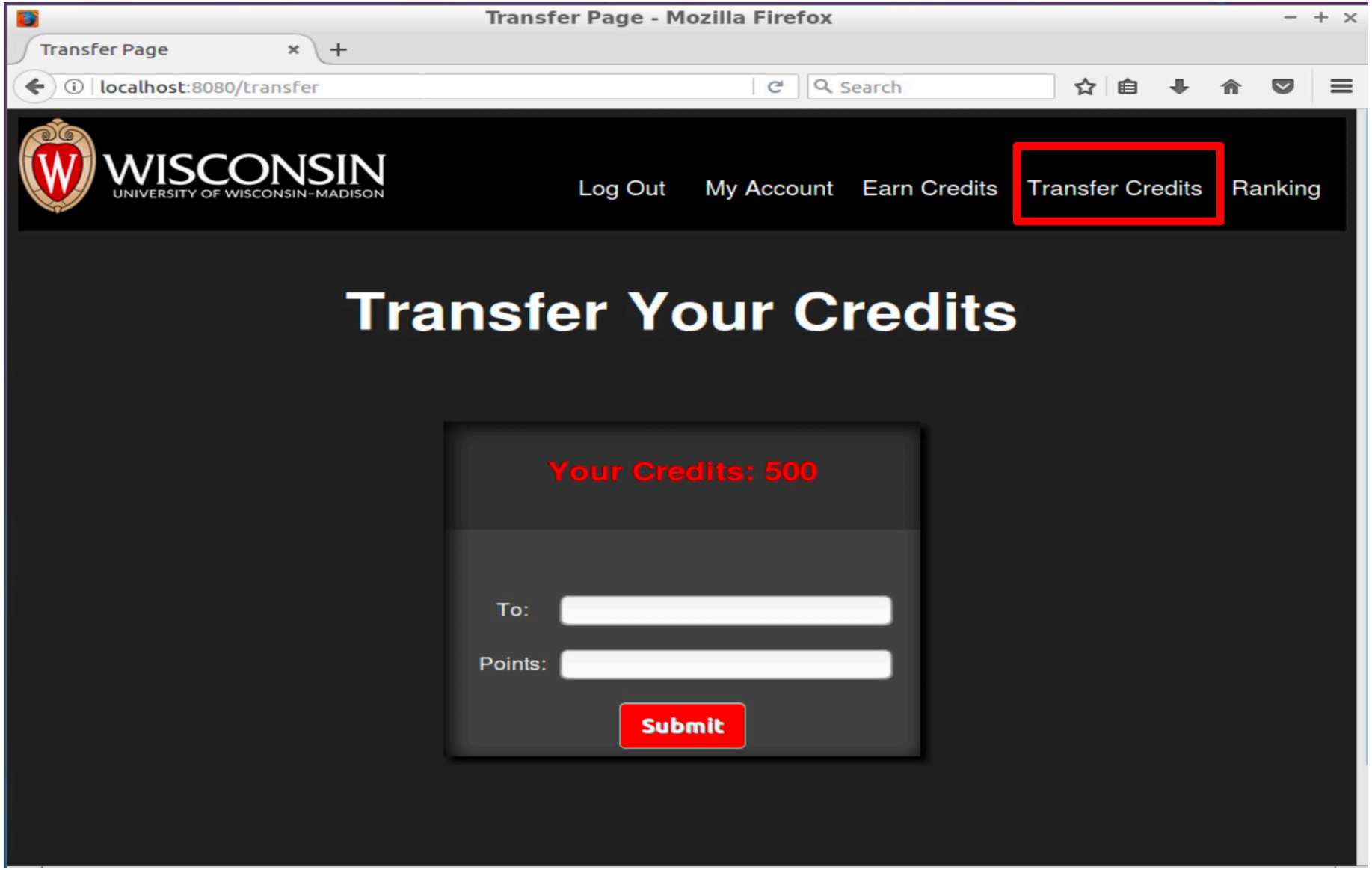
Run WisClick



Run WisClick



Run WisClick



WisClick Vulnerabilites

1. Cross-Site Scripting (XSS).
2. Cross-Site Request Forgery (CSRF).
3. Extracting Credentials and using them.

3. Extracting and Using Credentials

A. Send the victim's session id cookie to the attacker

Hint:

- **The attacker sets up a local server and listens to port 8000. In a console type:**

```
python -m SimpleHTTPServer 8000
```

- **The victim's cookies will be sent to that port.**
- **Craft your attack script in the `My Profile` field of the attacker's page.**
- **When the victim views the attacker profile, the attacker gets the session id cookie on the console.**

3. Extracting and Using Credentials

B. The attacker uses the stolen session id to steal the victim's credits.

In Web Inspector observe the cookies on the client side.

- After you log in the JSESSIONID cookie contains your session id.
- When you navigate trough WisClick, the browser will attach the cookies for that site, including JSESSIONID to the requests sent to server.
- The server will validate your JSESSIONID, and you will be able operate as an authenticated user.

3. Extracting and Using Credentials

Log in as Attacker.

Use the JSESSIONID cookie you stole from the victim to impersonate them:

- **Send a POST request with the victim's JSESSIONID to transfer credits to the attacker.**
- **Use a Postman Client for this attack:**

```
cd ~/Postman/
./app/Postman
```

REST Client (REpresentational State Transfer)

- **Create a POST request and send it to the server. Remember that the request will send the cookies for that site.**

3. Extracting and Using Credentials

- In the browser log in as the attacker and see your new credit.
- In the browser log in as the victim and see the credit gone.

Web Exercises
Part 3: Session Stealing

Barton P. Miller

Computer Sciences Department
University of Wisconsin

bart@cs.wisc.edu

Elisa Heymann

Computer Sciences Department
University of Wisconsin
Universitat Autònoma de Barcelona

elisa@cs.wisc.edu

THE UNIVERSITY of WISCONSIN MADISON

Universitat Autònoma de Barcelona

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE